WHAT IS CLAIMED IS:

1. A method of screening incoming packets, comprising:

detecting a request to establish a connection from a first network to a packet data network;

detecting establishment of a tunnel, wherein the tunnel has a support node at each end of the tunnel, one of the support nodes being a gateway to the packet data network, wherein the tunnel is used to convey user traffic and the user traffic through the tunnel can have one or more associated firewall sessions on a firewall outside the tunnel;

detecting a tear down of the tunnel; and

sending a request to the firewall to clear the one or more firewall sessions..

2. The method of claim 1, wherein:

detecting a tear down of the tunnel includes detecting the tear down of a GTP tunnel within the first network.

3. The method of claim 1, further comprising:

stopping passage of packets to the first network originating from the packet data network and associated with a firewall session that is not on the firewall session list.

4. The method of claim 1, further comprising:

dropping packets originating from the packet data network and not associated with a firewall session identifier on the firewall session list.

5. The method of claim 1, wherein:

detecting the tear down of the tunnel includes detecting GTP delete tunnel request and response messages.

6. The method of claim 1, further comprising:

clearing the one or more firewall sessions from a firewall session list.

7. The method of claim 1, further comprising:

adding a firewall session to a firewall session list at a time when a new tunnel is created.

8. The method of claim 1, further comprising:

inspecting packets in the tunnel to detect firewall session information.

9. The method of claim 8, wherein:

determining at least one of a source address and a destination address of the packets in the tunnel.

10. The method of claim 1, wherein:

detecting establishment of the tunnel includes determining the one or more firewall sessions associated with the tunnel.

11. The method of claim 10, wherein:

detecting establishment of the tunnel includes determining two or more firewall sessions associated with the tunnel.

12. A method of screening incoming packets, comprising:

providing a connection from a first network to a packet data network including providing a GTP tunnel, wherein the GTP tunnel has a support node at each end of the GTP tunnel, one of the support nodes being a gateway to the packet data network;

detecting a tear down of the GTP tunnel; and

applying a policy to determine whether to request a firewall session clear at a Gi firewall.

13. The method of claim 12, wherein:

applying a policy includes waiting for a period for a reconnect event.

14. The method of claim 13, wherein:

applying a policy includes not requesting a firewall session clear when a reconnect event is received within the period.

15. The method of claim 12, further comprising:

inspecting the packets in the GTP tunnel to determine firewall session information.

16. The method of claim 12, further comprising:

determining at least one of a source address and a destination address of the packets in the GTP tunnel.

17. A method of screening incoming packets, comprising:

detecting an establishment of a firewall session between a mobile station logged onto a GPRS network and a system on a packet data network;

detecting an end to the firewall session; and

sending a request to a Gi firewall protecting the gateway support node from attacks from the packet data network to remove the firewall session from an associated firewall session list.

18. A method of screening incoming packets, comprising:

adding a firewall session identifier to a firewall session list when a new firewall session for user traffic coming from a GTP tunnel is created and when the user traffic does not belong to an existing firewall session;

receiving a message to indicate the firewall session is no longer active; and

indicating the firewall session is no longer active on the firewall session list.

19. The method of claim 18, wherein:

indicating the firewall session is no longer active on the firewall session list includes removing the active firewall session from the firewall session list.

20. The method of claim 18, wherein:

indicating the firewall session is no longer active on the firewall session list includes marking the firewall session as inactive on the firewall session list.

21. The method of claim 18, further comprising:

dropping packets associated with the no longer active firewall session.

22. A system for screening incoming packets, comprising:

a GTP firewall having a GTP communication module; and

a Gi firewall having a Gi communication module that is operable to receive an instruction from the GTP communication module to tear down a firewall session, a firewall session list and a tear down engine that removes inactive firewall sessions from the firewall session list when the tear down engine receives the instruction from the GTP communication module.

23. The system of claim 22, wherein:

the GTP firewall is operable to detect a GTP tunnel tear down.

24. The system of claim 23, wherein:

the GTP firewall is operable to detect a firewall session end.

25. The system of claim 22, wherein:

the GTP firewall includes a Gn firewall provided at a Gn interface.

26. The system of claim 22, wherein:

the GTP firewall includes a Gp firewall provided at a Gp interface.

27. The system of claim 22, wherein:

the GTP firewall is located on a device; and

the Gi firewall is located on the device.

28. A method of screening incoming packets, comprising:

providing a connection from a GPRS network to a packet data network including providing a GTP firewall between support nodes in the GPRS network and a Gi Firewall between a support node operating as a gateway to the packet data network and the packet data network;

detecting a network attack originating from the packet data network at the GTP firewall; and

signaling the Gi Firewall to alert the Gi Firewall of the attack.

29. The method of claim 28 wherein the packet data network is the Internet.

30. The method of claim 28 wherein signaling the Gi Firewall includes sending a message to the Gi Firewall.

31. The method of claim 28 wherein signaling the Gi Firewall includes sending a message to clear a session in the Gi Firewall.